REMARKS

Claims 1-4 and 17-28 were pending at the time of the last Office Action. Applicant has amended claims 1, 17, 23, and 26 and canceled claims 21, 22, 27, and 28. Thus, claims 1-4, 17-20, and 23-26 are now pending.

Applicant is filing an interview request along with this response.

The Examiner has rejected claim 26 under 35 U.S.C. § 112, second paragraph, as being indefinite. Applicant has amended the claim to address the Examiner's concern.

The Examiner has rejected under 35 U.S.C. § 103(a) claims 1-4 and 23-25 based on Baugher, Minhazuddin, and Devine and claims 17-22 and 26-28 based on Baugher, Minhazuddin, Devine, and Dacosta. Although applicant disagrees, applicant has amended the claims to clarify the claimed subject matter.

Applicant has amended the claims to clarify that the packet or datagram received from a client includes only an encrypted version of a synchronization source identifier. For example, claim 17 recites "each packet not including an unencrypted synchronization source identifier but including an encrypted synchronization source identifier." A difficulty with prior techniques for sending packets that may include encrypted data is that the synchronization source identifiers were not encrypted. For example, Baugher's Figure 1 on page 6 illustrates the format of a packet. Figure 1 indicates that the encrypted portion is the "payload." (See to the left of the payload.) The synchronization source identifier is, however, not encrypted. Because the synchronization source identifier of Baugher is not encrypted, if the packet is transported through device that is untrustworthy (e.g., infected with a virus), the synchronization source identifier may be stolen by malware. The malware can use the synchronization source identifier to promulgate an attack on the destination client by sending malicious packets that include the synchronization source identifier. By

including only an encrypted synchronization source identifier in a packet, applicant's technology helps prevent such attacks. With applicant's technology, if a packet is intercepted by malware, the malware could use the source information that is unencrypted to launch an attack on the destination. However, when the destination receives the packet from such an attack, it will detect that the synchronization source identifiers do not match (except possibly for the first use of the packet) and discard the packet—thus mitigating any negative consequences of the attack.

Baugher uses a synchronization source identifier and the destination information of the packet to identify a cryptographic context. (Baugher, p. 10.) Since applicant's synchronization source identifier is encrypted, applicant's technology cannot use it to identify the security association associated with packet. To overcome this problem, applicant's technology uses unencrypted source information (e.g., sending client's source address and source port) included in the packet to identify the security association. Each of the claims has been amended to clarify that the unencrypted source information of the packet is used to identify the security association. For example, claim 17 recites "the source information of the sending client including an unencrypted source address" and "when no security association has been established that includes the source information." None of the relied-upon references teaches or suggests using the source address to identify a security association or cryptographic context. Indeed, Baugher teaches to explicitly use the destination address. (Baugher, p. 10.)

Once applicant's technology identifies the security association, it can then decrypt the packet synchronization source identifier and compare it to the established synchronization source identifier of the security association. If there is no match, applicant's technology discards the packet.

With applicant's technology, if a packet is intercepted by malware, the malware could steal the source information that is unencrypted and attempt to attack the

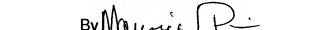
destination client. However, whenever the destination client receives the packet from such an attack, it will detect that the synchronization source identifiers don't match and discard the packet—thus mitigating any negative consequences of the attempted attack.

Based upon the above amendments and remarks, applicant respectfully requests reconsideration of this application and its early allowance. If the Examiner has any questions or believes a telephone conference would expedite prosecution of this application, the Examiner is encouraged to call the undersigned at (206) 359-8548.

Please charge any deficiencies or credit any overpayment to our Deposit Account No. 50-0665, under Order No. 418268874US from which the undersigned is authorized to draw.

Dated: March 31, 2009

Respectfully submitted,

By 

Maurice J. Pirio
Registration No.: 33,273
PERKINS COIE LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 359-8548
(206) 359-9000 (Fax)
Attorney for Applicant